Safeguard Computer Security Evaluation Matrix (SCSEM)

CA-Top Secret

Release IV

10-Dec-07

Tester: *Insert Tester Name*
Date: *Insert Date(s) Testing Occured*
Location: *Insert Location testing was conducted*
Agency POC(s): *Insert Agency interviewee(s) names*

Test ID	NIST ID (800-53/A)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments/Supporting Evidence
1	AU-2, AU-3, AC-17, SAMG-04	Audit trails are generated. Actions of any one or more users based on individual identity can be selectively audited.	Procedures: Obtain and review the audit and TSS violation reports distributed to and reviewed by the TSS analysts. If none, obtain and review the following TSS security reports. TSSAUDIT CHANGE – Logs updates to the security file report. TSSAUDIT CHANGE EVENT (VIOL) - Violation report. Password violation messages are always produced.	Expected Results: Each audit event trails the user and information relevant to the event (e.g., date and time of the event, user, type of event, file name and the success or failure of the event)			
2	AC-6	FTI datasets are restricted to users having a “need to know”.	Procedures: 1. Obtain the Access Rules (report) from the security officer for each FTI dataset. Note: The applications programmer or production control group may have to assist in identifying all FTI datasets. 2. Through inquiry of appropriate personnel, (data security, programming, data center operations) determine the name and job function of each user listed separately or within a group on the access control list. Determine whether users having access is appropriate and based on need to know and the least privilege concept. Given the nature of these datasets, even READ access may be inappropriate.	Users have access as appropriate and based on need to know and the least privilege concept.			
3	AU-2, AU-3, SAMG-04	Audit trails are generated for READ and above access attempts to FTI data sets.	Procedures: Determine data sets assigned the Audit attribute. Inquire of the administrator of the method for recording and auditing activities against FTI data sets. Obtain and review a sample of the audit reports.	Expected Results: FACILITY (LOG=DSN) Note:TSSUTIL - The security administrator determines the content of this report. The report shows detailed security related events. Note: The audit report records the date and time of the security events, the user, and the type of event/commands performed by privileged users.			

4	AC-3, AU-2, AU-3, SAMG-07	Powerful utility functions are logged and audited.	Procedures: Review the TSS MODIFY(STATUS) system Control Option report to verify that audit logs are capturing security related events. Default LOG=(MSG,SMF,INIT,SEQ9) Note: The LOG option identifies the types of events to log. MSG- violation messages SMF-location of event logs INIT-job initiations and terminations SEC9-batch job and STC violations FACILITY suboption overrides the global LOG option.	Expected Results: Audit logs are capturing security related events			
5	IA-3, PMG-01, PMG-09, PMG-17	Minimum password length is set at 8 characters. Password expiration warning is 5-14 days before the password change interval is enforced. Repeating characters are prevented for passwords. Password restriction list is actively enforced. Passwords are prevented from including the ACID.	Procedures: From review of the TSS MODIFY(STATUS) report verify that the NEWPW system Control Option is set to force strict passwords controls.	Expected Results: NEWPW(MIN=8,WARN=5,NR,RS,ID,TS,SW, FA,FN) Note:NR can also be represented as NR=0. RS operand points to the restricted password list. ID operand prohibits the use of passwords that are similar to the ACID. TS operand prohibits the use of a password that is too similar to the previous password. SW operand requires the use of a national character. FA operand requires the use of at least one alpha character. FN operand requires the use of at least one numeric character.			
6	IA-2, PMG-16	Passwords are required for all user logonids	Procedures: Review the list of interactive user accounts with the SA. Verify that all interactive user accounts have the PASSWORD field defined.	Expected Results: -All interactive users have a logon password defined in their user record.			
7	IA-3, PMG-02, PMG-03	Users are forced to change passwords at least every 90 days.	Procedures: From review of the TSS MODIFY(STATUS) report verify that the PWEXP(nn) system Control Option is set to force passwords to expire at least every 90 days. Note: The value should be 60 days for privileges user accounts (systems programmers, etc.)	Expected Results: PWEXP(90)			

8	AC-2, AC-7, PMG-10	Users' accounts are revoked after three (3) consecutive, unsuccessful login attempts.	Procedures: From review of the TSS MODIFY(STATUS) report verify that the PTHRESH(nn) system Control Option supports lockout after 3 unsuccessful attempts.	Expected Results: PTHRESH(3)			
9	IA-3, PMG-06	Passwords cannot be reused for 6 generation.	Procedures: From review of the TSS MODIFY(STATUS) report verify that the PWHIST (nn) system Control Option retains 7 generations of passwords history.	Expected Results: PWHIST(6)			
10	IA-3, PMG-17	Use of dictionary words, popular phrases, or obvious combinations of letters and numbers in passwords is prohibited	Procedures: Review the TSS MODIFY(RPW(LIST)) report	Expected Results: TSS MODIFY(RPW(LIST)) Note: TSS provides a list of 133 password prefixes that cannot be used as passwords. This list of common words supports the NEWPW(RS) system control options.			
11	PMG-07	Users shall be prohibited from changing their passwords for at least 15 days after a recent change. Meaning, the minimum password age limit shall be 15 days after a recent password change. Passwords cannot be changed for 6 generation.	Procedures: From review of the TSS MODIFY(STATUS) report verify that the NEWPW system Control Option is set to require password retention.	Expected Results: NEWPW(MINDAYS=15)			
12	IA-2, PMG-12, PMG-13	Started Tasks possess unique ACIDs and passwords.	Procedures: Review the TSS LIST(STC) DATA(ALL) report to determine whether STC possess unique ACIDs and passwords and do not share ACID with users.	Expected Results: All Started Tasks have unique userids and passwords			
13	AC-1, AC14	Access control policies governing the use of BYPASS command is adequate.	Procedures: Verify that policies and procedures are established to ensure: (1) Use of BYPASS command is restricted to authorized personnel and approved by appropriate systems management personnel; and (2)Use of the BYPASS command is monitored regularly.	Use of BYPASS command is restricted to authorized personnel, approved by appropriate systems management personnel; and is monitored regularly.			

14	AU-2, SAMG-16	Changes to the security file are recorded to the recovery file.	Procedures: From the TSS MODIFY(STATUS) report verify that the RECOVER system Control Option is set to record changes to the security file.	Expected Results: RECOVER(ON)			
15	AC-11	All dial-up access to the system is protected with approved devices or techniques that provide explicit identification and authentication and audit trails.	Procedures: Consult with the system administrator and verify that dial-up access is controlled through security measures.	Expected Results: DIAL-UP COMMUNICATIONS ARE ENCRYPTED.			
16	AC-11, AC-5	Access control in the form of properly administered user name and authentication shall be established for each user having dial-in access.	Procedures: Consult with the system administrator and verify that dial-up access is controlled through identification and authentication and audit trails.	Expected Results: DIAL-UP ACCESS REQUIRES USER IDS AND PASSWORDS OR HARDWARE TOKENS. DIAL-IN ACCESS IS RECORDED IN AUDIT LOGS.			
17	PMG-18	Users shall commit passwords to memory, avoid writing passwords down and never disclose passwords to others (e.g., with a co-worker in order to share files).	Procedures: Interview the IAM. Verify that policies and training are in place to ensure that users protect passwords appropriately. If possible, walk through the office areas and ensure that passwords are not written down (e.g. look for sticky-notes, passwords taped to keyboard bottoms, etc.)	Policies and training are in place to ensure that users protect passwords appropriately.			
18	PMG-15	Passwords shall not be automated through function keys, scripts or other methods where passwords may be stored on the system.	Procedures: Interview the IAM. Verify that policies and training are in place to ensure that users understand that passwords will not be automated or stored in clear text on the system.	Policies and training are in place to ensure that users understand that passwords will not be automated or stored in clear text on the system.			
19	PMG-12	Default vendor passwords shall be changed upon successful installation of the information system product.	Procedures: Interview the SA and IAM. Verify that procedures are in place requiring that default passwords for installed products are changed as part of the installation process.	Default passwords for installed products are changed as part of the installation process.			
20	SM-2	Ensure firmware and hardware components of the system are routinely reviewed using internal diagnostic software.	Procedures: Obtain understanding of the OS platform environment and review procedures used to perform routine diagnostic checks and maintenance on the system firmware and hardware components.	Firmware and hardware components of the system are routinely reviewed using internal diagnostic software			

21	AC-5, AC-6	Procedures: System security management controls are organized in a hierarchical manner, to allow the delegation of security management responsibility. Delegated authority is granted in the most restrictive fashion possible.	Procedures: Obtain and review the TSSCHART utility program to obtain the ACID structure for the organization. Obtain an organization chart. Review the TSSCHART report to determine which ACIDs are assigned security authorities: MSCA - Master Security SCA - Security Admin ZCA - Zone Security Admin VCA - Division Security Admin DCA - Department Admin LSCA - Limited Scope Admin Compare the TSSCHART report to the documented organization chart to determine adequacy of security authorities and identify conflicts of interest. Is security administered independently of application systems, technical support operations, and computer operations? Note: These capabilities should only be granted to a small group of users (ACIDs) with assigned security responsibilities	The security controls posture allows appropriate security privileges in a manner consistent with granting the least privilege necessary to allow security functions to be performed at the organizational level.			
22	AC-6	Users are prevented from circumventing key attributes.	Procedures: Obtain and review the TSSAUDIT report using the keyword "PRIVILEGES" for a listing of privileged ACIDs that allows users to bypass security attributes.	Expected Results: Evaluate all ACIDs with ADMIN authority. Ensure that all personnel with ADMIN have data security responsibilities. Evaluate all ACIDs with the following attributes. CONSOLE NOADSP NODSNCHK NOLCFCHK NOPWCHG NORESCHK NOSUBCHK NOVOLCHK			
23	AC-6	Data sets and general resources are controlled from global access.	Procedures: Review the TSS LIST(ALL) DATA (ALL) report to verify that data sets and general resources global ALL record privileges do not provide users with additional unnecessary authority.	Data set and general resources global ALL record privileges do not provide users with additional unnecessary authority.			

24	CM-3	Activate security bit for new data sets in an Alwayscall environment.	Procedures: From the TSS MODIFY(STATUS) report verify that the ADSP(xx) system Control Option is set properly.	Expected Results: ADSP(NO) (Note: An Alwayscall environment requires ADSP(NO).) ADSP(NO) - will not turn on the security bits for newly created data sets in non-Alwayscall environment. ADSP(NO) - Vendor default setting			
25	CM-3	Ensure the authorization (AUTH) search criteria supports the organization's security configuration.	Procedures: Interview the security administrator to gain an understanding of the organization security configuration. From the TSS MODIFY(STATUS) report verify that the AUTH system Control Option is set securely to YES.	Expected Results: AUTH(OVERRIDE) AUTH(OVERRIDE,ALLOVER) - Vendor default setting Note: AUTH indicates whether TSS will merge the User, Profile, and ALL records when performing access authorization search, or whether TSS will search each record separately. OVERRIDE presents security concerns because the first authorization identified during the search is accepted. Therefore, if authorized at the User level and not permitted at the Profile level, then the user will be granted access. MERGE is acceptance as it searches as one continuous record. The ATTR definition allows the search criteria to be defined at the data set and supersede the global AUTH setting.			
26	CP-4, SAMG-16	The Security File is automatically and periodically backed up to allow for an expeditious and accurate recovery security privileges.	Procedures: From the TSS MODIFY(STATUS) report verify that the BACKUP(xx) system Control Option is set to automatically backup the Security File.	Expected Results: BACKUP or BACKUP(hhmm) BACKUP immediately backups up the Security File. BACKUP(hhmm) backups up the Security File daily at the time specified. BACKUP(0100) - Vendor default setting Note: Either recommendation will periodically backup the Security File. Note: This setting is dependent upon the BACKUP DD statement being present/ defined in the TSS started task procedure.			

27	AC-6	Jobs and users are prevented from circumventing and bypassing TSS security software controls.	Procedures: From the TSS MODIFY(STATUS) report verify that the BYPASS system Control Option is set to control jobs and users according to the TSS privileges.	Expected Results: BYPASS - Should not be specified. Note: If it is specified (only the MSCA can do this), you must get explanation from the security administrator as this allows the specified ACID or job to bypass TSS controls. BYPASS is not a vendor default setting.			
28	AC-6	Jobs and users are restricted from accessing resources and data when the TSS package becomes inactive.	Procedures: From the TSS MODIFY(STATUS) report verify that the DOWN(Sx,Tx,Bx,Ox) system Control Option is set to control jobs and users when TSS becomes inactive.	Expected Results: DOWN(SB,TW,BW,OW) Note: If Top Secret becomes inactive, only started tasks may bypass security (SB). Other facilities must wait (xW). There can be more than four entries, investigate all entries suffixed "B" (bypass). S = Started Tasks T = TSO B = Batch O = Online DOWN(SB,TW,BW,OW) – Vendor default setting			
29	AC-5	Security administrators are prevented from overriding certain security violation activities.	Procedures: From the TSS MODIFY(STATUS) report verify that the DRC system Control Option is set to control ACID from overriding certain security violation activities.	Expected Results: DRC(IN,DS,VL,RS,PW) Note: DRC - Use should be documented as this allows security administrators to change the characteristics of Detailed Reason Codes, errors codes) IN- selects all initiation violation codes. DS- selects all data set violation codes. VL- selects all volume violation codes. RS- selects all resource violation codes. PW- selects all password violation codes. DRC is not set as a default value.			
30	AC-5, SAMG-17	Security administrators are prevented from overriding certain security violation activities.	Procedures: From the TSS MODIFY(STATUS) report verify that the EXIT(xx) system Control Option is set to control ACID from overriding certain security violation activities.	Expected Results: EXIT(ON) Note: Defining the TSSINSTX in the link-list will also activate the EXIT feature.			

31	CM-3	Control Options specific to critical facilities are securely defined to prevent users from circumventing TSS controls.	Procedures: From the TSS MODIFY(STATUS) report verify that the FACILITY (e.g.,APPC, TSO, CICS, BATCH, STC,IMS) Control Options are set to control activities. Review Facility Control Options to determine whether they conflict with the Global Control Options or support sound security practices. Control options for consideration include: LOGGING, LOCKTIME, MODE, & LOCKTIME.	Expected Results: MODE=FAIL DOWN=WAIT or DOWN=FAIL LOCKTIME=030 Note: Facility Control Options supersede Global Control Options. Use guidance provide in the Global Control Options presented above. DOWN=NORMAL provide native system security when TSS is inactive. Generally, not an acceptable level of security. DOWN=GLOBAL defaults to the setting defined by the DOWN control option. An asterisk (*) has the same meaning as GLOBAL. This is an acceptable definition only if the aforementioned DOWN control option is adequately defined. Locktime is available for on-line facilities, and note that individual locking thresholds can be set by users/profiles that override the facility level threshold values.			
32	AC-5	Only system programming personnel are authorized to access sensitive and critical SYS1 data sets	Procedures: Obtain and review the TSS WHOHAS DSN(SYS1.*) report to determine adequacy of the data profile. Note: Access to the SYS1 high-level qualifier should be restricted to a limited number of system programming personnel.	Access to the SYS1 high-level qualifier should be restricted to a limited number of system programming personnel.			
33	AC-5	Only system programming personnel are authorized to update the SYS1.PARMLIB concatenation.	Procedures: Obtain and review the TSS WHOHAS DSN(SYS1.PARMLIB) report. Determine appropriateness of defined ACID and ACCESS parameters. Note: ACCESS- option provides universal privileges to users.	Expected Results: Access to the SYS1.PARMLIB partition data set should be restricted to a limited number of system programming personnel.			
34	AC-5	Only system programming personnel are authorized to update the SYS1.UADS data set.	Procedures: Obtain and review the TSS WHOHAS DSN(SYS1.UADS) report.	Expected Results: Access to the SYS1.UADS partition data set should be restricted to a limited number of system programming personnel.			

35	AC-6	Users cannot modify the ALTER, CONTROL or UPDATE access authority to the SMF audit files (e.g. SYS1.MAN*).	Procedures: Obtain and review the TSS WHOHAS DSN(SYS1.MAN*) report.	User have no access to the SYS1.MAN* data sets			
36	AC-6	UPDATE and ALLOCATE authority will be restricted for the APF library.	Procedures: Obtain and review access report for all APF and APF LNKLST library DSNs to determine properly controlled.	Expected Results: UPDATE (Read/Write access) and ALLOCATE authorities are restricted for these APF library DSNs. TSS WHOHAS DSN(SYS1.CMDLIB) TSS WHOHAS DSN(SYS1.CSSLIB) TSS WHOHAS DSN(SYS1.LINKLIB) TSS WHOHAS DSN(SYS1.LPALIB) TSS WHOHAS DSN(SYS1.MIGLIB) TSS WHOHAS DSN(SYS1.PARMLIB) TSS WHOHAS DSN(SYS1.SVCLIB) TSS WHOHAS DSN(SYS1.UADS) TSS WHOHAS DSN(SYS1.VTAMLIB)			
37	AC-6	Access to sensitive libraries is properly restricted.	Procedures: Obtain and review the TSS WHOHAS DSN(xxx.x) (TSS.SECFILE) - Security File (TSS.AUDIT) - Audit/Tracking File (optional alternate file) (TSS.BACKUP) - Backup File (TSS.RECOVERY) - Recovery File (TSS.CMP) - Command Propagation Files	Expected Results: Only a limited number of individuals should have access to these records.			
38	AC-6	Access to sensitive TSS libraries are properly restricted.	Procedures: Obtain TSS primary and secondary data sets name and review the TSS WHOHAS DSN(xxx.x) report to determine that the Owners are not individuals and the locations are different volumes.	Access to sensitive TSS libraries are properly restricted.			

39	CM-3	Entries residing in the MVS Program Properties Table (PPT) are configured in accordance with IBM recommendations.	Procedures: Review the TSSAUDIT Program Properties Table Report and identify programs that: (1) bypass TSS password protection; and (2) reside in a system key.	Expected Results: Ensure the aforementioned programs are configured in accordance with vendor recommendations.			
40	CM-3	Tape security is activated.	Procedures: Review the TSS MODIFY(STATUS) system Control Option report to verify tapes security is activate.	Expected Results: TAPE(ON) or a tape management product (CA-1) is in use.			
41	AC-8	All computer systems must have an IRS-approved screen-warning banner that outlines the nature and sensitivity of information and the consequences /penalties for misuse.	Procedures: Obtain and review the Warning Banner for compliance with IRS guidance.	Expected Results: The warning banner is compliant with IRS guidelines. The warning banner should indicate users are subject to monitoring and are subject to penalties and prosecution. Sample Warning Banner Text is: UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both. All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials.			

42	SC-2	All FTI residual information is erased from the DASD volume.	Procedures: From the TSS MODIFY(STATUS) report verify that the AUTOERASE(xx) system Control Option is set securely to YES	Expected Results: AUTOERASE(YES) AUTOERASE(NO) - Vendor default setting Note: AUTOERASE(YES) is mandatory to achieve the DOD C-2 level of certification or higher. Note: AUTOERASE(YES) - Forces TSS to write binary zeros into the space occupied by VSAM and non-VSAM data sets when they are deleted. This erases all residual information on the DASD volume. YES is valid only in IMPL and FAIL modes. Therefore, from the TSS MODIFY(STATUS) report, determine whether the MODE setting supports the AUTOERASE control option.			
43	SC-3, SC-8, SC-9, SC-13	FTI is encrypted while traversing networked, or interconnected systems from remote locations.	Procedures: Obtain a network diagram that depicts all access points used to process, store and transmit FTI – noting firewalls, routers, and switches where applicable. Determine if IP traffic (TN3270 terminal emulation sessions used to access application functions that process FTI, FTI file uploads/downloads) containing FTI is encrypted when traversing communication lines (e.g. T1, T3, ISDN) using encryption solutions including, but not limited to: Triple DES, SSL, TLS, or Secure IP Tunneling (VPN using IPSEC). Evaluate viable encryption alternatives for appropriateness.	IP traffic (TN3270 terminal emulation sessions used to access application functions that process FTI, FTI file uploads/downloads) containing FTI is encrypted when traversing communication lines (e.g. T1, T3, ISDN) using approved encryption solutions.			
44	AC-11	The information system prevents further access to the system by initiating a session lock after [an organization-defined time period] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	Confer with the IAM and SA. Verify that interactive sessions (TSO, TPX, etc.) are locked after a period of inactivity in accordance with IRS guidelines. The inactivity time should be 15 minutes or less.	Interactive sessions are locked after the requisite period of time.			

45	AC-12, SC-10	The information system automatically terminates a remote session after [an organization-defined time period] of inactivity. (1) Automatic session termination applies to local and remote sessions.	Confer with the IAM and SA. Verify that interactive sessions (TSO, TPX, SSH, etc.) are terminated after a period of inactivity in accordance with IRS guidelines.	Interactive sessions are terminated after the requisite period of time.			
46	AC-13, AU-5	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. (1) The organization employs automated mechanisms to facilitate the review of user activities.	Confer with the IAM. Verify that procedures are in place to review audit logs on a regular, periodic basis, and that these procedure are followed (i.e. that the reviews are performed). Inquire whether automated data review and reductions tools are available and/or in use.	Audit logs are reviewed on a regular basis. Automated tools are used if available.			
47	AC-17	The organization authorizes, monitors, and controls all methods of remote access to the information system. (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. (3) The organization controls all remote accesses through a limited number of managed access control points. (4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan	Confer with the IAM and SA. Determine how remote accesses are managed and controlled. If remote execution of privileged functions (administration, etc.) is permitted, ensure that such privileges are properly justified and documented. Ensure that remote sessions are properly encrypted.	Remote accesses are properly justified, documented, managed and controlled.			

48	AU-4	The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	With the systems programmer, review the size of the SYS1.MANx files, the %-utilization, and the schedule with whish the files are dumped (backed up) and cleared.	SYS1.MANx files are managed adequately to prevent the loss of system audit data.			
49	AU-5	The information system alerts appropriate organizational officials in the event of an audit processing failure	With the systems programmer, ensure that the system issues console alerts when the SYS1.MANx files approach critical threshold. Verify that the operations staff has standing instructions to notify the appropriate personnel, and that procedures have been established to dump the SMF data.	Appripriate console alerts are issued, and procedures exist to notify personnel and to manage the backup of SMF data.			
50	AU-7	The information system provides an audit reduction and report generation capability.	Confer with the IAM and the SA to determine what SMF data audit reduction and reporting tools are available (in addition to standard z/OS SMF reporting mechanisms.)	Data reduction tools are available and in use.			
51	AU-8	The information system provides time stamps for use in audit record generation. (1) The organization synchronizes internal information system clocks [Assignment: organization-defined frequency].	Confer with the Systems Programmer and IAM to determine the site policy and procedures for setting, verifying, and synchronizing the system clock. Inquire whether the system clock is set to GMT+0 with a Time Zone offset, or whether the system clock is set to local time.	Policy and procedures exist for setting and periodically synchronizing the system clock. Note: Audit data (SMF) time stamps should reflect GMT time.			
52	AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Determine in which library (SYS1.LINKLIB, etc.) the system audit data reporting tools reside. Obtain a TSS WHOHAS report for the library, and for SYS1.MAN*. Identify personnel who have access to the files and utilities. Ensure that no personnel have excessive access permissions.	Access to the SYS1.MANx filies and reporting tools is restricted to the appropriate personnel.			
53	AU-11	The organization retains audit records for [an organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Confer with the Systems Programmer and IAM to determine the site policy and procedures for dumping (backing up) SMF data and creating duplicate backups to prevent data loss. Determine that the site data retension policy is in accordance with IRS guidelines.	Policy and procedures exist for backing up and retaining SMF data.			

54	IA-4	The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [an organization-defined time period] of inactivity; and (vi) archiving user identifiers.	Confer with the IAM to deterimine the site policy and procedures for issuing, managing, revoking, and archiving user access credentials. Determine whether or not logon IDs are re-issued after they have been used.	The site should have adequate procedures in place to issue, manage, revoke, and archive user access credentials. User logon IDs should not be re-issued to new personnel once they have been used.			
55	IA-5	The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	Confer with the IAM to deterimine the site policy and procedures for issuing and disseminating initial user passwords, and for requiring and enforcing periodic system-wide password change.	The site should have adequate procedures in place for initial password dissemination and periodic system-wide password change.			
56	SC-2	The information system separates user functionality (including user interface services) from information system management functionality.	Interview the IAM and SA. Determine whether privileged users have separate accounts for performing day-to-day user activities than those used for performing privileged functions/tasks.	Privileged personnel should not use the same logon IDs for both normal and priveleged functions.			

57	SC-5	The information system protects against or limits the effects of denial of service attacks. (1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks. (2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	Interview the IAM, SA, and Network Systems personnel. Determine what capabilities the system has to detect and prevent inbound and/or outbound flooding-based denial of service attacks	The system should provide protection against flood-type denial of service attacks.			
58	SC-23	The information system provides mechanisms to protect the authenticity of communications sessions.	Interview the IAM, SA, and Network Systems personnel. Determine what capabilities the system has to prevent network session hijacking	The system should provide protection against network session hijacking.			
59	SAMG-16/17	The audit trail shall be protected from unauthorized access, use, deletion or modification. The audit trail shall be restricted to personnel routinely responsible for performing security audit functions.	Procedures: 1. Request the System Administrator to generate a TSS data set access report. Review the report and verify that access to the SMF data sets (SYS1.MANx) is restricted to authorized personnel.	Access to the SMF data sets (SYS1.MANx) is restricted to authorized personnel.			
60	SAMG-1--15	Auditing is configured to capture security-relevant events.	Procedures: 1. Review SYS1.PARMLIB(SMFPRMxx) 2. Ensure that, at a minimum, all IBM (00-127) and TSOMON (199) SMF record types are written. (Top Secret uses the RACF SMF record types.) Request documentation for any record types appearing in a NOTYPE(nn) parameter. 3. If SMF exits IEFU83, IEFU84, IEFU85 are listed, verify with the Systems Programmer the functions performed by the exits. Ensure that they do not suppress required SMF record types. 4. Verify that the system SMF data sets (SYS1.MANx) exist and are written to.	1. IBM (00-127) and TSOMON (199) SMF record types are written. . 2. Documentation exists for any record types appearing in a NOTYPE(nn) parameter. 3. If SMF exits IEFU83, IEFU84, IEFU85 are listed, they do not suppress required SMF record types. 4. The system SMF data sets (SYS1.MANx) exist and are written to.			

61	SAMG-1	The audit trail shall capture all successful login and logoff attempts.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 30, 32 IBM: 80 (used by TSS)	The required data are collected.			
62	SAMG-2, SAMG-3	The audit trail shall capture all unsuccessful login and authorization attempts. The audit trail shall capture all identification and authentication attempts.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 80 (used by TSS)	The required data are collected.			
63	SAMG-5	The audit trail shall capture all actions, connections and requests performed by privileged functions	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 32	The required data are collected.			
64	SAMG-6	The audit trail shall capture all changes to logical access control authorities (e.g., rights, permissions).	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 80 (used by TSS)	The required data are collected.			
65	SAMG-7	The audit trail shall capture all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 90[-9], 90[-10] IBM: 80 (used by TSS)	The required data are collected.			

66	SAMG-8	Access to FTI is audited. The audit trail captures the creation, modification and deletion of objects including files, directories and user accounts. Pub 1075 5.6.2 states, “Security-relevant events must enable the detection of unauthorized access to FTI data.”	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 17, 18, 19, 59, 60, 62, 63, 64, 67, 68, 69, 83, 92 IBM: 80 (used by TSS)	The required data are collected.			
67	SAMG-9	The audit trail shall capture the creation, modification and deletion of user accounts and group accounts.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 80 (used by TSS)	The required data are collected.			
68	SAMG-10	The audit trail shall capture the creation, modification and deletion of user account and group account privileges	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 80 (used by TSS)	The required data are collected.			
69	SAMG-11	The audit trail shall capture: i) the date of the system event; ii) the time of the system event; iii) the type of system event initiated; and iv) the user account, system account, service or process responsible for initiating the system event.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 90	The required data are collected.			

70	SAMG-12	The audit trail shall capture system startup and shutdown functions.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 0, 22[-1]	The required data are collected.			
71	SAMG-13	The audit trail shall capture modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-equivalent account(s); and ii) adding or deleting users from the administrator group account(s).	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 80 (used by TSS)	The required data are collected.			
72	SAMG-14	The audit trail shall capture the enabling or disabling of audit report generation services.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 23	The required data are collected.			
73	SAMG-15	The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, database).	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 22, 32, 83, 101, 110 IBM: 80 (used by TSS)	The required data are collected.			

IRS Safeguard SCSEM Legend

Test Case Tab: Execute the test cases and document the results to complete the IRS Safeguard Computer Security review. Reviewer is required to complete the following columns: Actual Results, Comments/Supporting Evidence.

Test ID	Identification number of SCSEM test case
NIST ID	NIST 800-53/PUB 1075 Control Identifier
Test Objective	Objective of test procedure.
Test Steps	Detailed test procedures to follow for test execution.
Expected Results	The expected outcome of the test step execution that would result in a Pass.
Actual Results	The actual outcome of the test step execution, i.e., the actual configuration setting observed.
Pass/Fail	Reviewer to indicate if the test case pass, failed or is not applicable.
Comments / Supporting Evidence	Reviewer to include any supporting evidence to confirm if the test case passed., failed on not applicable As evidence, provide the following information for the following assessment methods: 1. Interview - Name and title of the person providing information. Also provide the date when the information is provided. 2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible). Ensure all supporting evidence to verify the test case passed or failed. If the control is marked as NA, then provide appropriate justification as to why the control is considered NA.